RESILIENZA ORGANIZZATIVA ALLE MINACCE DELLO SPAZIO CYBER

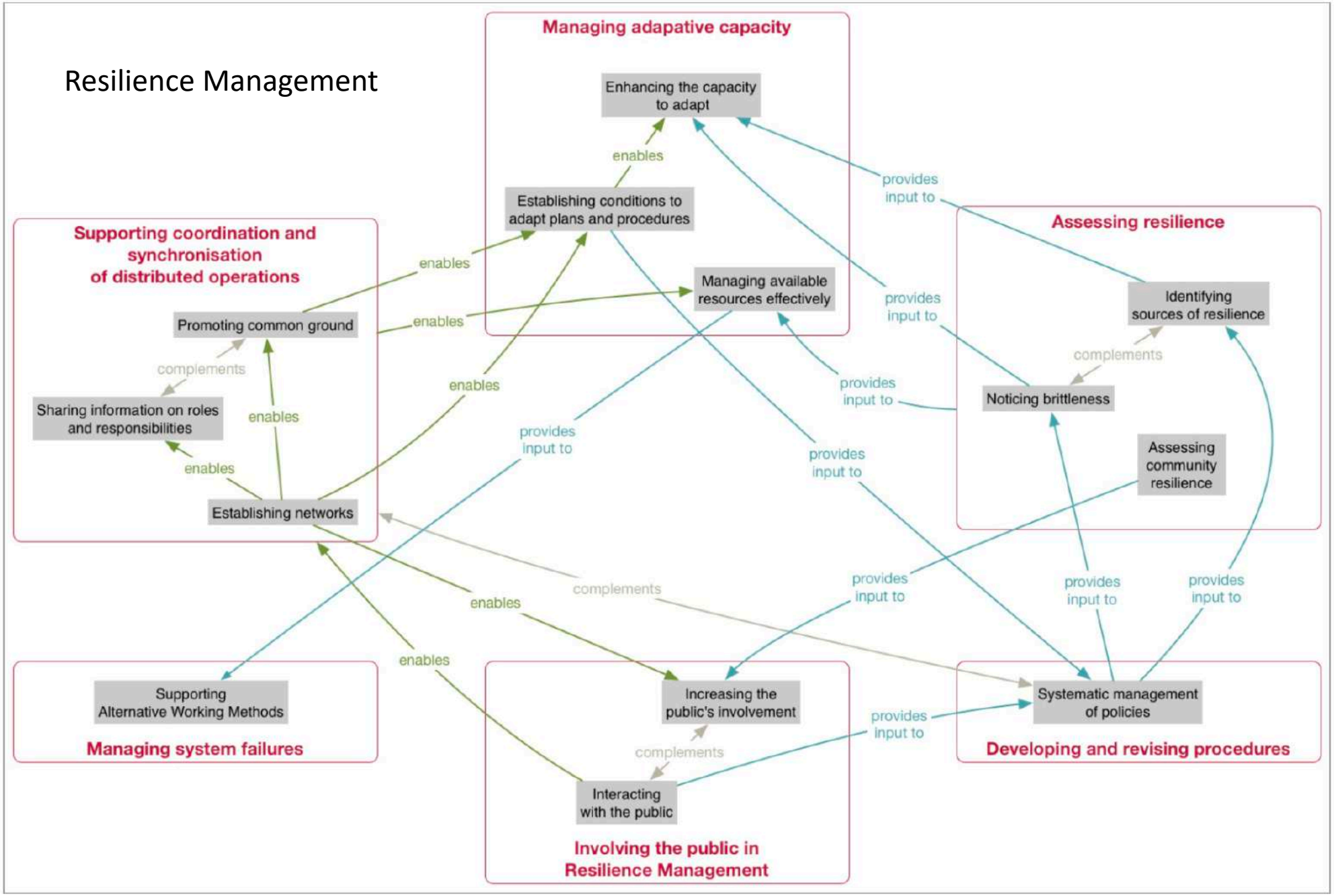
Paolo Spagnoletti, Luiss University e Competence Center Cyber 4.0

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

LUISS

Fonte: adattato da World Economic Forum Global Risks Perception Survey 2016–2020

Resilience Management



https://h2020darwin.eu/

Theoretical background: NAT VS HRO

NORMAL ACCIDENT THEORY

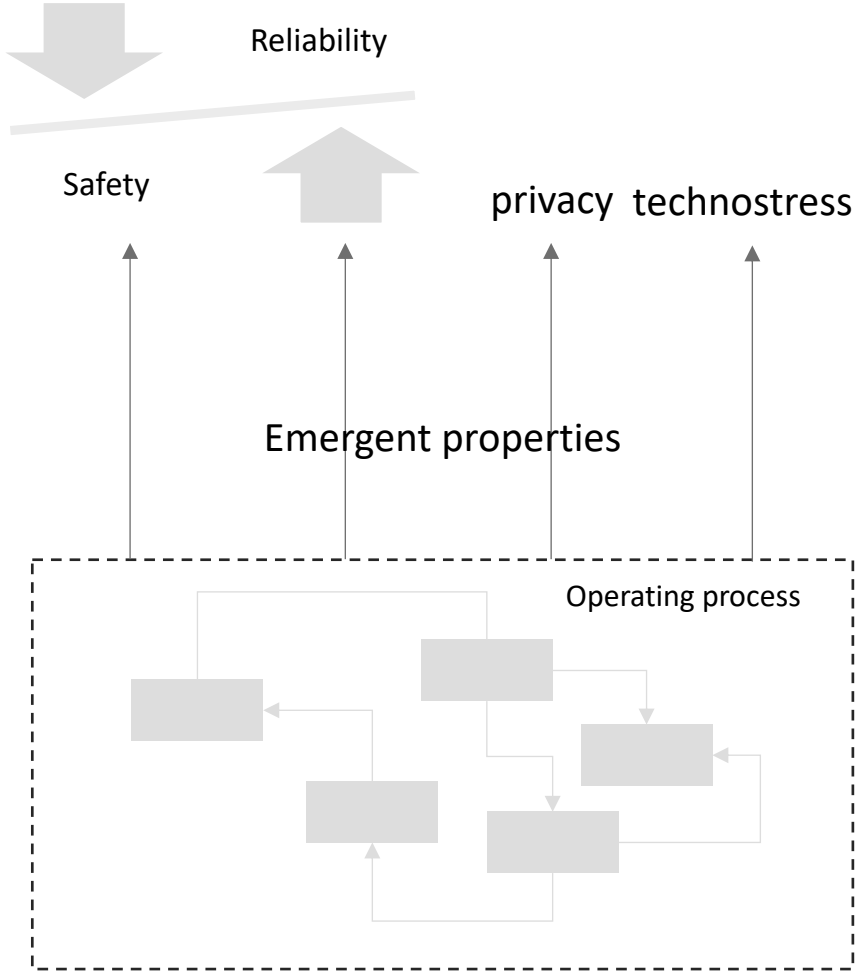
- Interactive complexity and tight coupling of technological systems
- Localized failures spread/disrupt/damage larger systems
- System accidents are inevitable or “normal”

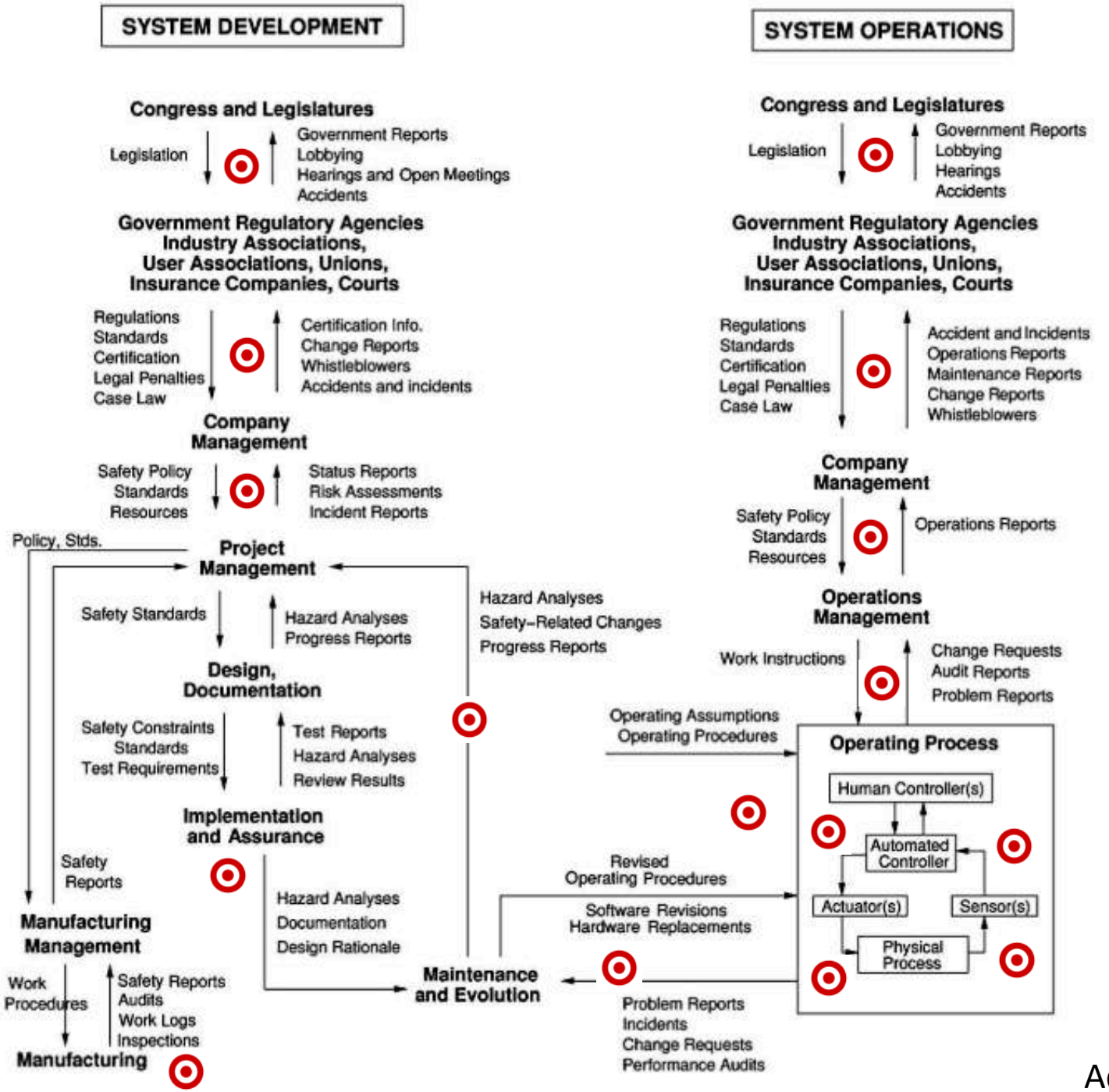
HIGH RELIABILITY ORGANIZATIONS

- Hallmarks
  - Preoccupation with failure
  - Reluctance to simplify
  - Sensitivity to operations
  - Commitment to resilience
  - Deference to experience
- Safety enacted on the front lines during crisis

A SYSTEM APPROACH TO SAFETY

- Complexity: interactive, structural, dynamic, etc.
- Coupling: time, control, data or information, structural, etc.
- Hazard: event (or condition) being avoided
- Engineering design: search for optimal/acceptable tradeoffs between engineered system properties, physical limitations and various system objectives (e.g. performance)
- Accidents caused by dysfunctional interactions instead than component failure





Cyber-physical attacks

Adapted from Leveson et al. 2009

Le sfide per le organizzazioni

- Preparare le organizzazioni a rispondere alla minaccia cyber integrando
  - Crisis management: fragmented coordination
  - Resilience: multi-level operational control
- Strumenti di difesa
  - Scenario based training for situational understanding
  - Agile architecture maintenance and evolution
  - Active defense: digital twins, sandboxes, AI, etc.

Riferimenti

- Baskerville, R., Spagnoletti, P., and Kim, J. 2014. “Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response,” *Information & Management* (51:1), pp. 138–151.
- Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. Organization Studies, 30(2–3), 227–249. https://doi.org/10.1177/0170840608101478
- Spagnoletti, P., Ceci, F., and Bygstad, B. 2018. “The Generative Mechanisms of Dark Net Markets,” in *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, December 13*, pp. 1–15.
- Marchetti, R., and Mulas, R. 2017. Cyber Security: Hacker, Terroristi, Spie e Le Nuove Minacce Del Web, Roma: LUISS University Press.

Grazie per l’attenzione

pspagnoletti@luiss.it

http://www.linkedin.com/in/pspagnoletti